Analysis of APT-C-60 Attack on South Korea

linkedin.com/pulse/analysis-apt-c-60-attack-south-korea-threatbook/

ThreatBook

#ThreatBook Security Incident Analysis Report

Summary

APT-C-60 is disclosed by domestic security vendors in 2021. It is reported that the earliest attack time can be traced back to 2018 and the attack targets human resources and trade-related institutions including China. Recent monitoring by ThreatBook Intelligence Research and Response Team found that the Group has been active since December 2021. In June this year, the Group launched targeted attacks on targets in S. Korea. With analysis of the attacks, the findings are as follows:

- The targets of this batch of attacks include Dr. Bernhard Seliger, the representative of the Hanns Seidel Stiftung, and politicians who may be related to the 2022 Pyeong Chang Peace Forum.
- Two time nodes of this attack: attack on the politicians related to the 2022 Pyeong Chang Peace Forum in early February 2022; targeted attack on Dr. Bernhard Seliger in mid-June 2022. Both are spear-mail type attacks.
- The network assets used by attacker for payload hosting attack and C&C communication include public free cloud storage sites (such as bitbucket.org, statcounter.com) and attacker private C&C assets. Trojan back link address is to involve multiple url addresses of these two types.
- ThreatBook extracts multiple related IOCs though the traceability analysis of related samples, IPS, and domain names, which can be used for threat intelligence detection. TDP, TIP, API, OneDNS, OneEDR of ThreatBook have all supported the detection of this attack activity and group.

Details

On June 20, 2022, the spear-mail delivered to seliger@hss.de is as follows. The attacker pretended it to be a Korean graduate student’s thesis defense to induce the target person to download malicious files hosted on cloud.mail.ru.

图片无替代文字

The downloaded file is a rar compressed file, containing bait file and malicious lnk files. The bait files related to the thesis are as follows (The Chinese environment of the office causes the Korean to display abnormally).

图片无替代文字

According to the machine ID in the Lnk file attribute information: desktop-iag9k61, we also found attack on the early stage of the Pyeong Chang Peace Forum in February 2022 by APT-C-60. The bait file used is as follows.

图片无替代文字

In the two attacks, the bitbucket.org site used for payload hosting and file uploading included user IDs: grand9_neat, Miravos, sorakas. Storage files related to the current attack have been deleted.

图片无替代文字图片无替代文字图片无替代文字

Sample Analysis

The payload execution process in the attack is as follows. Starting from the downloaded compressed file, the persistence payload is to be divided into three parts: Lnk file with malicious download, downloader Trojan (mssysmon.db) with file information acquisition and download execution, remote-control Trojan (TaskControler.dll) with file stealing, plug-in loading, and shell function. Subsequent sections are to analyze the three types of components.

图片无替代文字

Malware Lnk

Taking “Online questionnaire-Exploring ways to cooperate with North Korea.docx.lnk” as an example, the sample information is as follows

图片无替代文字

The command-line of Lnk file is as follows. Call mshta to execute remote javascript.

图片无替代文字

Javascript resource jumps through the html index code.

图片无替代文字

Obfuscated javascript code after the jump is as follows.

图片无替代文字

This js code downloads the next-stage malicious resource from the C&C server , decrypts it and then moves it to %appdata%\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db.

图片无替代文字

From the download file retrieval code, the existing default download file extensions include “.dib”, “.bmp”. Currently C&C can only download bmp files.

图片无替代文字图片无替代文字

By jacking the COM object whose CLSID is 603D3801-BD81-11d0-A3A5-00C04FD706EC, the persistence of the landing Trojan is realized. The CLSID is bound to the service named “shared task scheduler”, which is related to Windows scheduled tasks, and its registered dll component is loaded when os starts.

图片无替代文字

mssysmon.db

Taking “mssysmon.db” as an example to analyze, the sample information is as follows.

图片无替代文字

Analyze the landing mssysmon.db file, which is dll file, and the core function is provided by tdstart export function. Before running Trojan, control the unique instance running by creating an event object named “673304C7B2797C3676B6”.

图片无替代文字

Decrypt the C&C configuration, which contains multiple URL address. The Trojan heartbeat interval is 6 hours.

图片无替代文字

The Trojan creates the %AppData%\Microsoft\HTML Help directory as the directory for subsequent plug-in distribution and log storage. The Trojan acquires the host name, username, os version, and uses AEC encryption to send it to C&C server to go online. AES key is “8394M8YRRNK2EJRA” in the previous decryption configuration file.

图片无替代文字

Traverse c:\Program Files\ directory, acquire file directory information, and send it to the C&C server. C&C target address includes two as follows: http://162.222.214.50/temp/sourcea.php, https://c.statcounter.com/12733057/0/f9b868f1/1/.

图片无替代文字

Traverse the %AppData%\Microsoft\HTML Help directory, delete the .mui file and load msiobj.dll file. If the msiobj.dll file does not exist, then download it again. The download address includes: http://185.207.206.108/premium/P1/HTBXTDQJJHMI.bmp, https://bitbucket.org/grand9_neat/well/downloads/19132.bmp, https://bitbucket.org/grand9_neat/well/downloads/19164.bmp.

图片无替代文字

The loading logic in the %AppData%\Microsoft\HTML Help directory is as follows. Rename the downloaded and decrypted msiobjs.dll to msiobj0.dll, and then load and call msiobj0.dll!ExtFunc. if it fails, change the dll extension to mui, and delete the mui file.

图片无替代文字

TaskControler.dll

Taking “TaskControler.dll” as an example to analyze, the sample information is as follows.

图片无替代文字

The Trojan is a 64-bit dll component developed by C++. TaskControler.dll!extension provides core function.

图片无替代文字

In the initialization phase of the C++ object, start “83a078f58a078f7a88f37g0gf8a873a8” to perform the “xor 2 -1” operation to obtain the RC4 key “90b149c69b149c4b99c04d1dc9b940b9”, which is to be used for the encryption and decryption of the communication field in the subsequent C&C communication.

图片无替代文字

Before running the Trojan, control the unique instance running by using the mutex “9ABKD3409ABACL6SGHDG404HNJ0”.

图片无替代文字

Open the %AppData%\Roaming\Microsoft\Vault\UserProfileRoamings directory. If it does not exist, create the directory and set it to be hidden.

图片无替代文字

After that, the Trojan traverses the %AppData%\Roaming\Microsoft\Vault\UserProfileRoamings directory ，and runs the attack payload in this directory according to the file extension.

图片无替代文字图片无替代文字

Decrypt C&C 160.20.147.118. Send https://api.ipify.org/ request to obtain the internet IP. Acquire information of host and user into the core Trojan work logic. When it is detected and judged that the system has been started for more than 6 hours, the main thread is to go online with C&C, set a ten-minute heartbeat interval, and schedule working thread by event object signals.

图片无替代文字

The working thread is composed of five independent threads which respectively complete the corresponding functions: task request, result feedback, screen monitoring, file stealing, RAT.

图片无替代文字

The debugging environment Trojan online packet is as follows.

图片无替代文字

The data in the body with the form of "a001=*&a002=*&a003=*&a004=*" is partially parsed as follows.

图片无替代文字

There are also post data packets of “b001=*&b002=*&b003=*&b004=*”, “c001=*&c002=*&c003=*&c004=*” type in the Trojan communication, which respectively represent to parse the URL issued by the C&C for downloading action and file uploading.

In the file uploading part, there are some differences in the processing of screenshot files and file content: the screenshot files are encoded by base64 and converted to decimal strings; the file content is first encrypted with RC4 and then converted to decimal strings.

图片无替代文字图片无替代文字

By parsing C&C commands, the RAT distribution thread can achieve the functions such as file directory traversal, disk information acquisition, process termination, DLL loading, screenshot, downloading, process execution, file or directory deletion and cmd shell.

图片无替代文字图片无替代文字

The full RAT parsing is as follows.

图片无替代文字

Support encrypted file download. The download file landing path is temp%\wcts66889.tmp, which needs to be decrypted by AES. AES128 key={21 A4 47 12 68 5A 8B A4 29 85 78 3B 67 88 39 99}。

图片无替代文字

The C&C receives shell, transfers it through the local named pipe “\\.\pipe\async_pipe”, and then executes it starting with cmd.

图片无替代文字

Association Analysis

This sample is basically the same as the execution process of the landing payload in the previous APT-C-60 attack. The third-stage component TaskControler.dll is the same as the historical attack with same export function and same code behavior and communication process. The following figure is a screenshot of the historical attack time analysis of the APT-C-60, in which the forgery payload component directory and payload traversal loading logic in the DLL payload export function “extension”, “%AppData%\Roaming\Microsoft\” are exactly the same. Therefore, it is more credible to attribute this attack sample to APT-C-60.

图片无替代文字Quoted from https://www.secrss.com/articles/36606

Appendix - IOC

C2

131.226.4.22:80

160.20.147.118:80

162.222.214.50:80

185.145.97.62:80

185.207.206.108:80

82.221.129.104:80

82.221.136.60:80

URL

http://185.145.97.62/temp/cheack.php

http://131.226.4.22/manager/JxQpe5T2nCn747UP.bmp

http://162.222.214.50/temp/sourcea.php

http://185.145.97.62/temp/cheack.php

http://185.145.97.62/cache/A1

http://185.145.97.62/cache/A2

http://185.207.206.108/premium/P1/WHZAZVRYVJTN.bmp http://82.221.129.104/k0201.txt

http://82.221.129.104/k0201jo.txt

http://82.221.136.60/ping/a22.txt

https://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/command.asp
https://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/result.asp
https://bitbucket.org/grand9_neat/well/downloads/19132.bmp
https://bitbucket.org/grand9_neat/well/downloads/19164.bmp
https://bitbucket.org:443/grand9_neat/well/downloads/19164.bmp
https://bitbucket.org/miravos/style/downloads/1932.bmp

https://bitbucket.org/miravos/style/downloads/1964.bmp

https://bitbucket.org/sorakas/mod/downloads/1932.bmp

https://bitbucket.org/sorakas/mod/downloads/1964.bmp

https://c.statcounter.com/12733057/0/f9b868f1/1/

https://c.statcounter.com:443/12733057/0/f9b868f1/1/

https://c.statcounter.com/12557354/0/adafe4e4/1/

https://c.statcounter.com/12557356/0/d8c85be6/1/

Hash

13f09fd98259e6636e523fb8254cf9e8b5c562605dbf826cf2fc3ae57ed09c77
266ee1b357cad72a1a9d0a1a6f7d3f0a53fce60b885ba0983a20d813c22b3009
74b34adf28552f380163346c151c7dfdcac70e5df2187374113b891e7740ad91
7c4fb90eeb997555dc5d4c1ccbe26a5ae1a3cda4ef5571eb3a83c4ac50ffd906
7ec34297e0c4e5b1bb315be24d7259211ab658112dc0f9d6d7271544f87244e0
92912bfb10b475958ab1bae510be6829c2eb11b8eb5fd365321db642457328da
9bb60e54c09934c559c7dc0bb0eb0527a7e2e066cd1c452ed4f4519025d1f9b0
a995f4e4e5bec985ea974dac2a65056e7ab9f2b80430d94857530bedef5e74f6
b2dd50760765abfbed0a7db480d4429228b165cb23b720d11abc4390c30a26fc
bc879fe3e928ca9c1de4b9a600716f2076e6ce371313255797fb312cf9f7dd04

bffacbb0b54a3b1dd6f25686d2486d0a064f5e8eedefb4e572740f7b63ba4fa4

dbc1754de49824d25ef6d9cc338512a61d56ec14363355e68acfc6f450c2c0e4
e869e82a9f44d81b272e53b449da7c8c4a667cf26dea8dee67086726ab22c500
edec420761cd95ba706c9f50f29bbb76786d5279c4ada162f513e0cb1fa4cf84
ee862a3d57e45a2b29da9e74987016061e225df71a558c6a42f0819cc7496664

f50cd82717837a5b5fb985c8f080fa3d5cabb05b146aed14e3810ae90fb37e01

File Path

%appdata%\Microsoft\Vault\UserProfileRoamings\

%appdata%\Microsoft\Vault\

%appdata%\Microsoft\Internet Explorer\UserData\

%AppData%\Microsoft\HTML Help\

To view or add a comment, sign in